

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE <b>23 OCT 2014</b>		2. REPORT TYPE <b>N/A</b>		3. DATES COVERED	
4. TITLE AND SUBTITLE <b>Insider Threat Mitigation Project: A Dynamic Network Approach</b>				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) <b>; Carley /Andrew P. Moore KathleenClaycomb /William</b>				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) <b>Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213</b>				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT <b>Approved for public release, distribution unlimited.</b>					
13. SUPPLEMENTARY NOTES <b>The original document contains color images.</b>					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT <b>SAR</b>	18. NUMBER OF PAGES <b>1</b>	19a. NAME OF RESPONSIBLE PERSON
a. REPORT <b>unclassified</b>	b. ABSTRACT <b>unclassified</b>	c. THIS PAGE <b>unclassified</b>			



# Insider Threat Mitigation Project

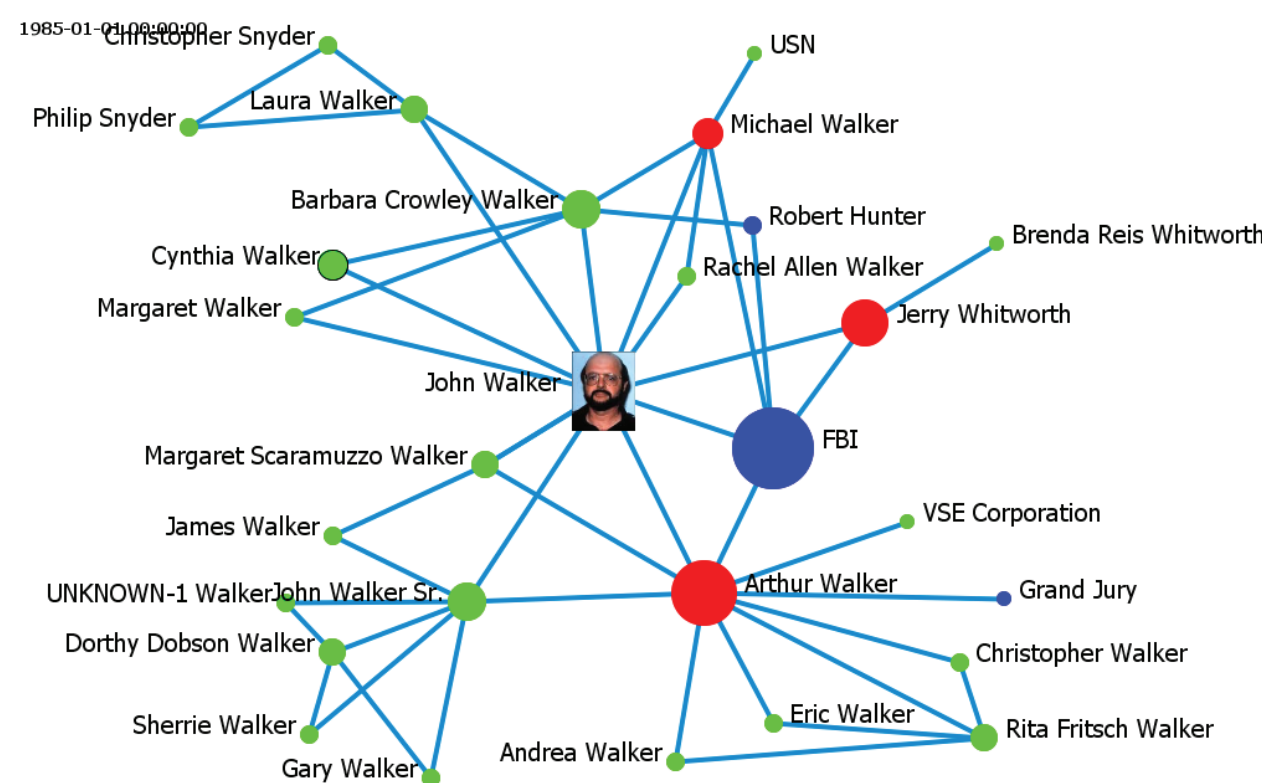
## A Dynamic Network Approach

### Emergence of Threat – Ego centered analysis of specific cases

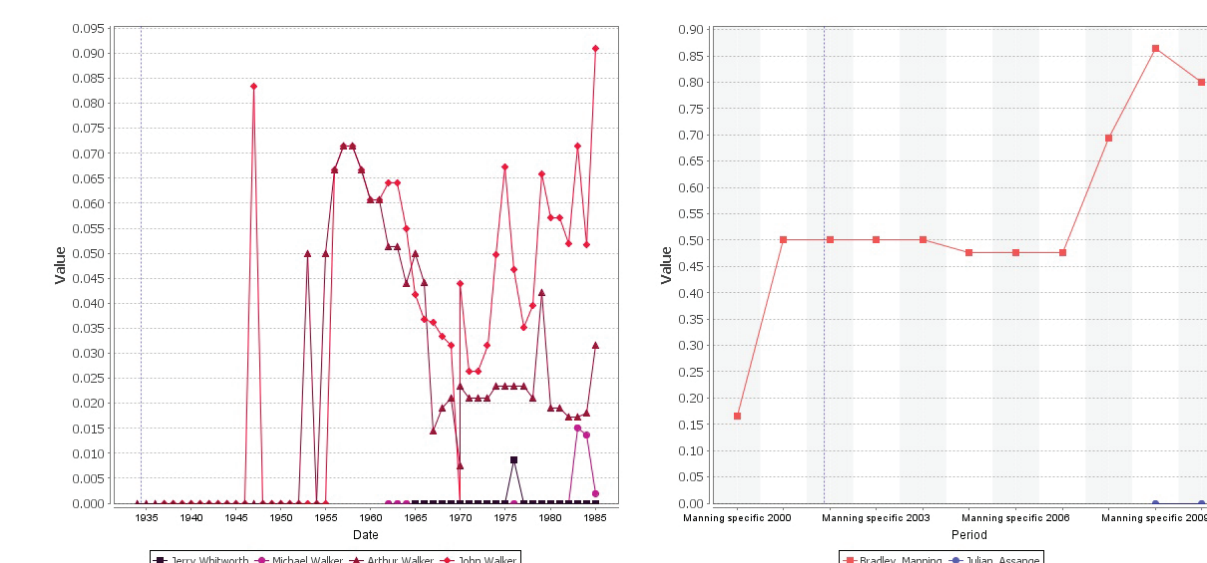
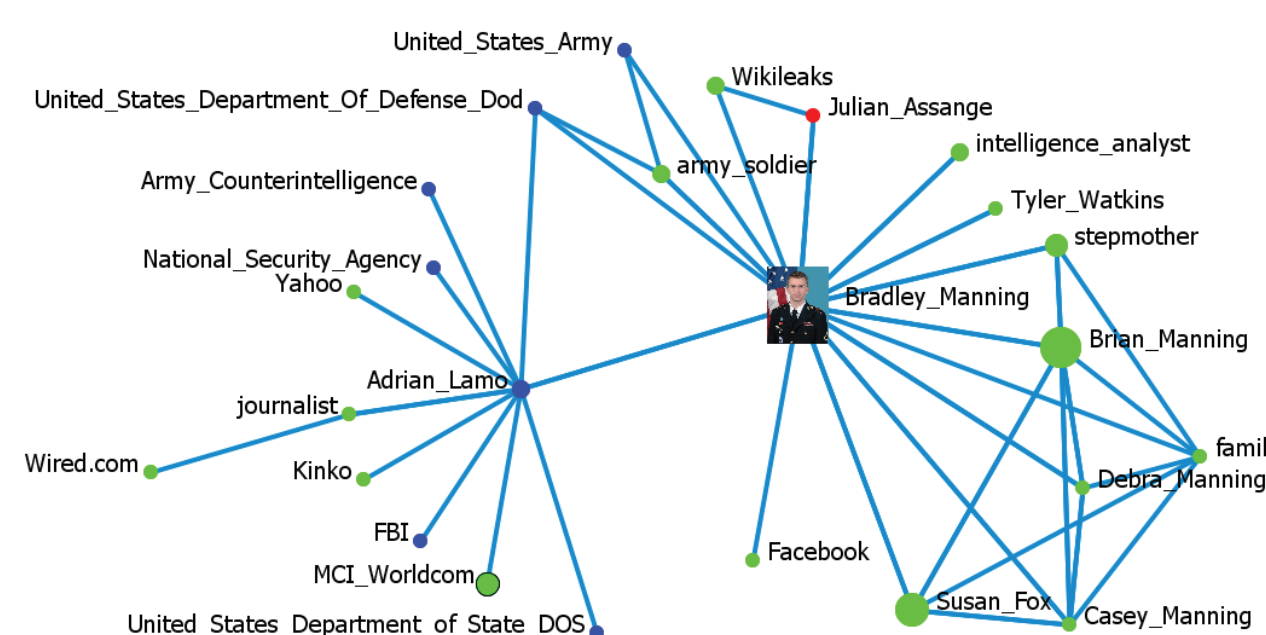
#### Approach:

- Semi-automated coding with fine-tuning to add dates
- Extract meta-networks one per year
- Comparison at “role” level
- Apply network analytics and visualization

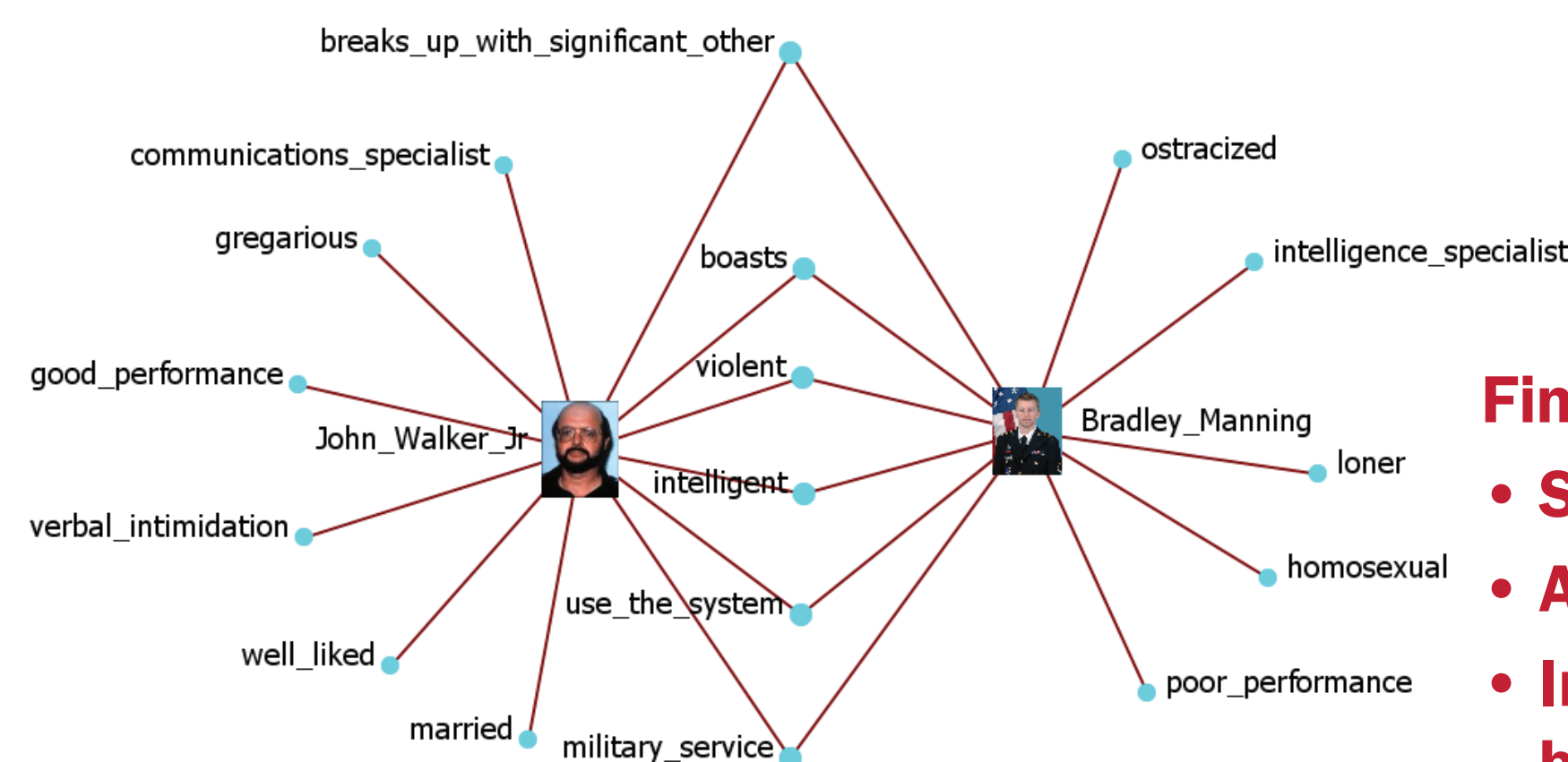
#### Walker – Gang example Case records/searches (open-source)



#### Manning – Lone Wolf example open-source



Increasing betweenness during spy activities



#### Findings on Insiders:

- **Special characteristics**
- **Access**
- **Increasing betweenness**
- **Disrupted family network**

### Emergence of Threat – Email centered analysis of possible anomalies

#### Approach:

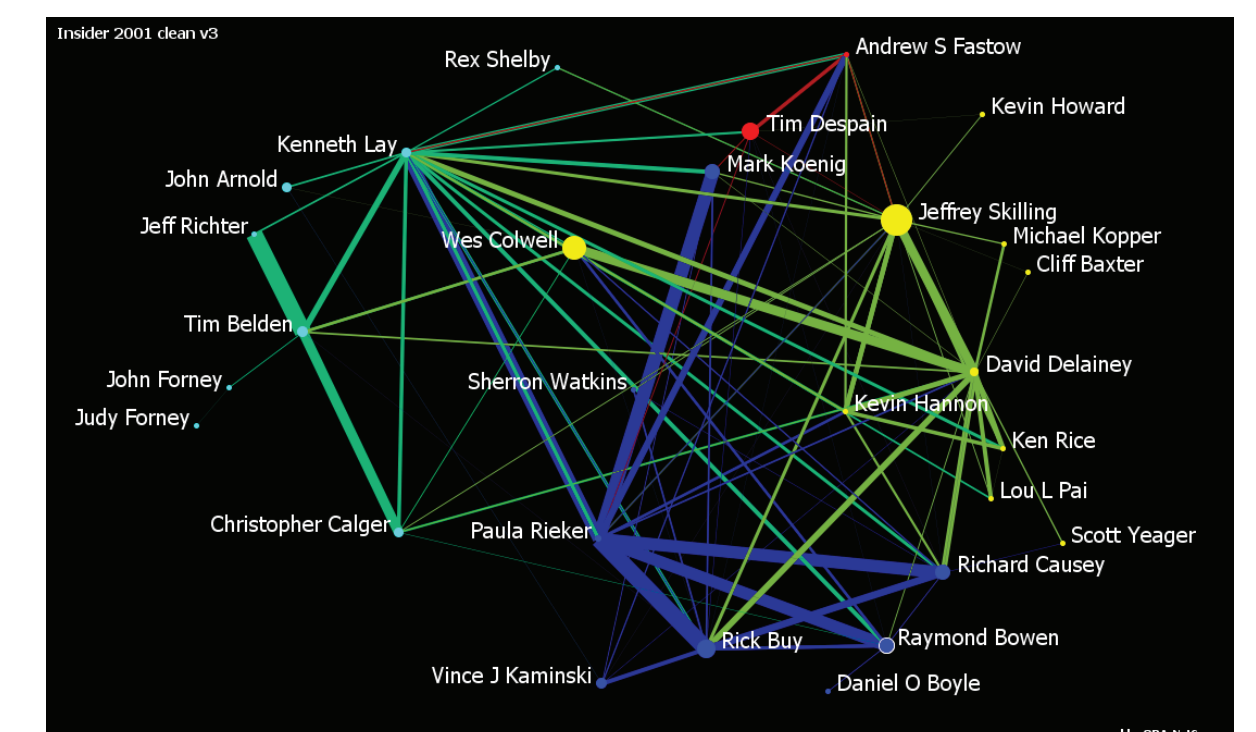
- Networks formed from meta-data
- One network per year
- Segment internal from internal-to-external communication
- Remove suspected distribution lists
- Identify “normal behavior” using Enron
- Develop pattern for “insiders” in contrast to “normal” using Enron
- Apply to anonymized SEI email

#### CMU-CS (and CASOS):

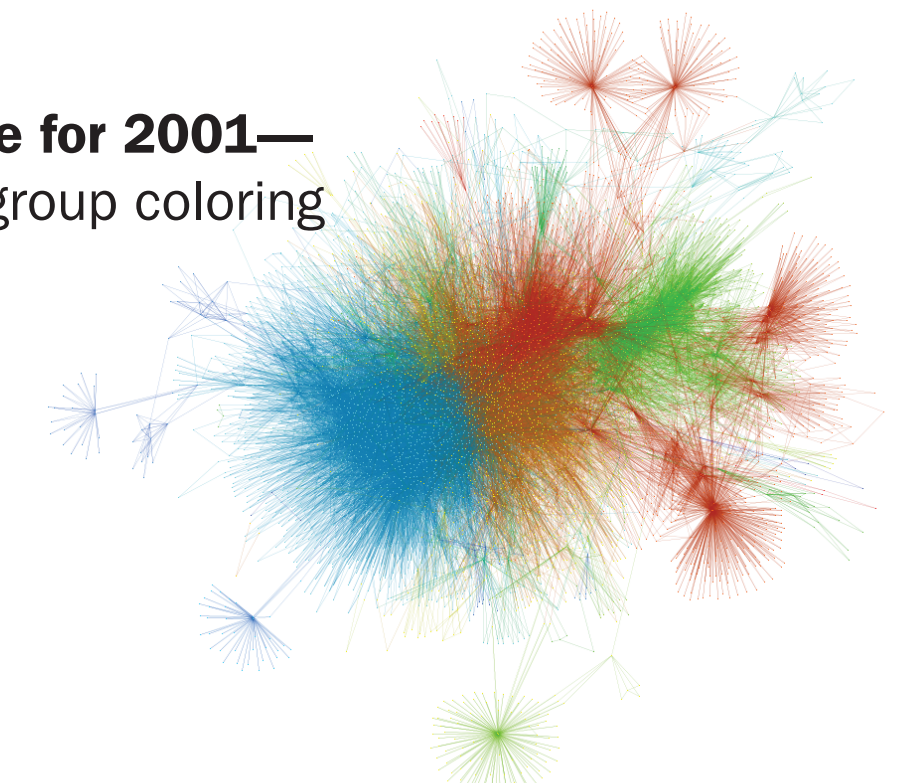
- Dr. Kathleen Carley
- Neal Altman
- Geoff Morgan
- Matt Benigni

#### SEI:

- Matthew Collins
- Andrew Moore
- Dr. William Claycomb



#### Enron core for 2001— Newman group coloring

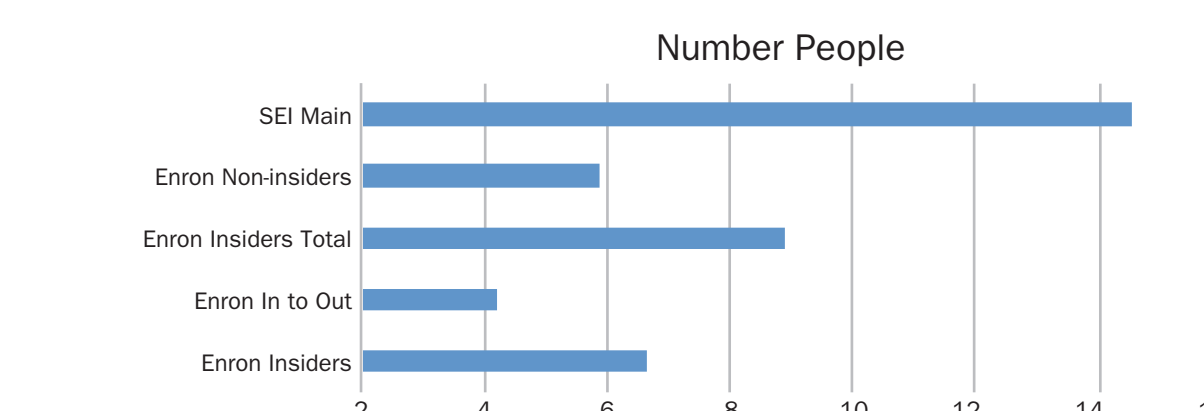
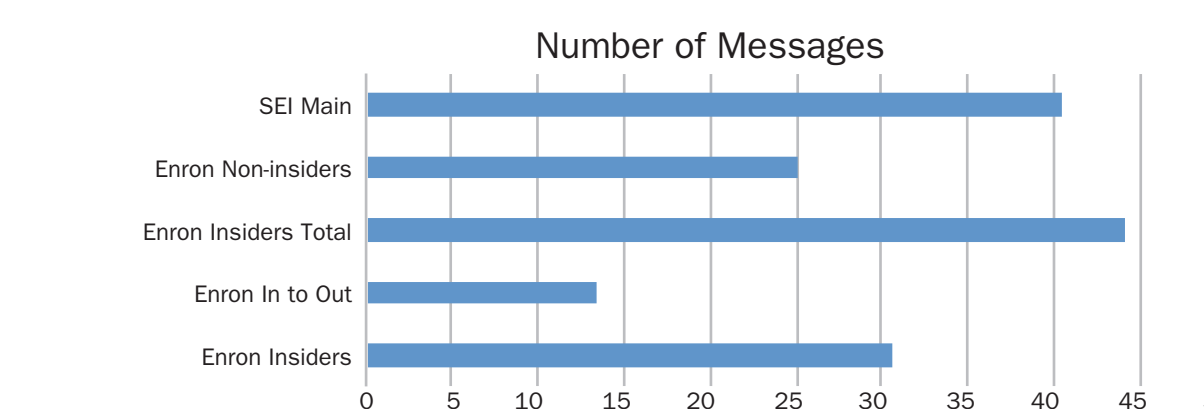
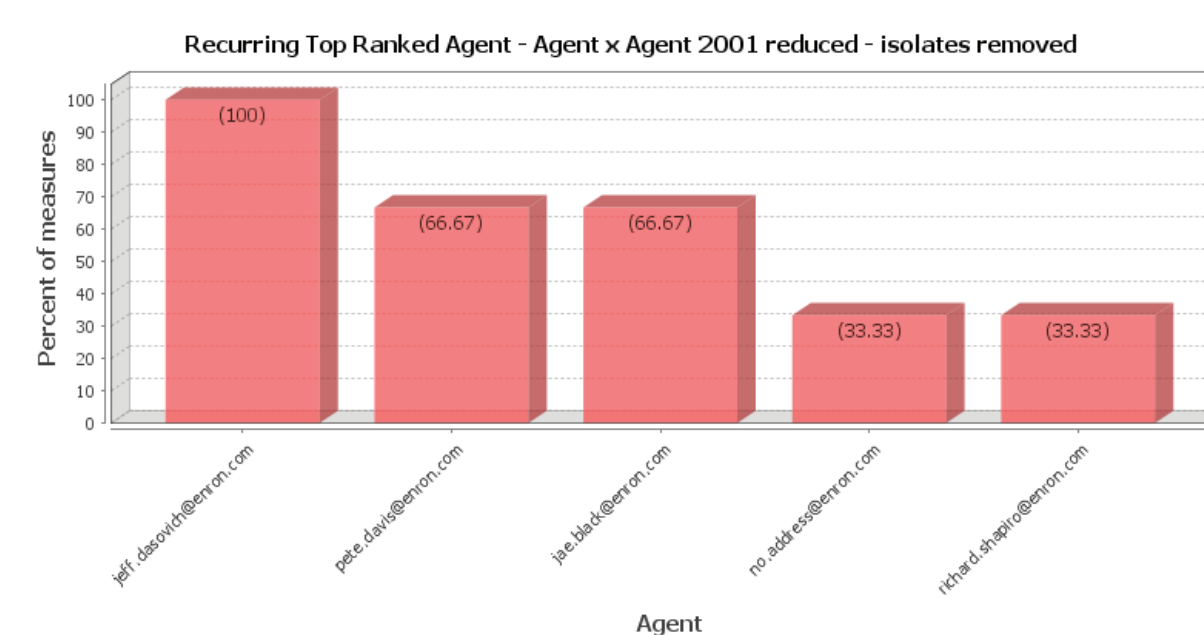


#### SEI core for 2013— Newman group coloring



#### Findings on “Insiders”— those accused:

- **Are not “top” network actors**
- **Form a densely connected sub-group**
- **High level of in-group communication**
- **Low out-group communication**



#### Findings on SEI -v- Enron:

- **SEI—more email, proportions similar**
- **Both—dominant dense core with numerous stars**